Technical Cybersecurity

Different NMAP Scans

Variety of Scans

PREVIOUS SCAN

- ARP requests only
- …we were on the same subnet.

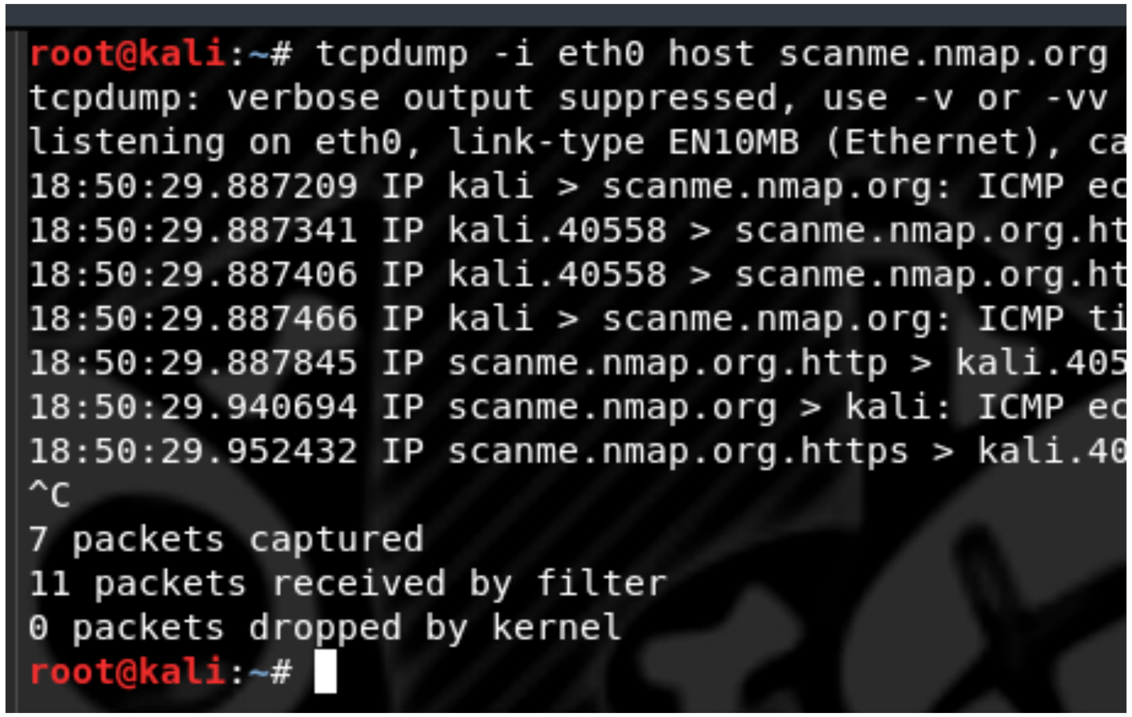
TRY A DIFFERENT HOST

- scanme.nmap.org
- **$ nmap -sP** scanme.nmap.org
- **$ tcpdump -i eth0 host** scanme.nmap.org

External Scan Different

NMAP EXTERNAL SCANS DIFFER

- Sends ICMP Echo Request (e.g. ping)
- Sends TCP ACK to 80
- Sends TCP SYN to 443
- Sends ICMP Timestamp Request



```
root@kali:~# tcpdump -i eth0 host scanme.nmap.org
tcpdump: verbose output suppressed, use -v or -vv
listening on eth0, link-type EN10MB (Ethernet), ca
18:50:29.887209 IP kali > scanme.nmap.org: ICMP ec
18:50:29.887341 IP kali.40558 > scanme.nmap.org.ht
18:50:29.887406 IP kali.40558 > scanme.nmap.org.ht
18:50:29.887466 IP kali > scanme.nmap.org: ICMP ti
18:50:29.887845 IP scanme.nmap.org.http > kali.405
18:50:29.940694 IP scanme.nmap.org > kali: ICMP ec
18:50:29.952432 IP scanme.nmap.org.https > kali.40
^C
7 packets captured
11 packets received by filter
0 packets dropped by kernel
root@kali:~# 
```

Scanning Options

VARIOUS SCAN OPTIONS

- -Pn or -P0 turns off
- -sP (sweep probe, we used this one)
- -PB (default), -PE (pings), -PS [ports] (SYN probe), -PP (timestamp request), -PM (address mask request), -PR (ARP scan)
- -sS (stealth or half-open scan, uses SYN packets)
- -F (fast, only top 100 ports)
- —top-ports [N] (N top ports)
- -T, -U (tcp, udp)
- -p [ports] (ports to scan)

Scanning Options

OTHER SCANNING OPTIONS

- -sP, -sS we know
- -sT (connect scan)
- -sA (ack scan, good for host ID, not for port open; good at going through filters though)
- -sF (FIN bit set on all packets)
- -sN (NULL control bits on packets)
- -sX (FIN, PSH, and URG)
- -sM (FIN and ACK bits)

Next: more examples!